UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

| | | |
|---|---|---|
| UNITED STATES OF AMERICA | ) | |
| v. | ) | CRIMINAL NO. 21-cr-10104-PBS |
| VLADISLAV KLYUSHIN<br>Defendant | ) | |

**DEFENDANT VLADISLAV KLYUSHIN'S RESPONSE TO GOVERNMENT'S OPPOSITION TO HIS MOTION TO SUPPRESS**

Now comes the defendant Vladislav Klyushin, by and through undersigned counsel, and hereby respectfully responds to the government's opposition to his motion to suppress. In a last-ditch effort to save three overbroad search warrants based on affidavits that failed to establish requisite probable cause, the government, in its opposition, improperly attempts to backfill Special Agent Kang's two affidavits to include facts and circumstances that were omitted from the initial applications. These new additions not only violate the long-standing principle that "review is limited to the 'facts and supported opinions' set out within the four corners of the affidavits," *United States v. Austin*, 991 F.3d 51, 55 (1st Cir. 2021), but are also, at times, inaccurate and unsupported. Moreover, these newly assembled assertions fail to justify Special Agent Kang's "beliefs" or his exclusion of damaging credibility revelations that undermined the agent's unsupported, speculative assertions in an affidavit otherwise lacking probable cause. Finally, the itemized categories contained within the warrants that the government relies on to justify its fishing expeditions are so vague that they provided no meaningful guidance to investigators attempting to distinguish responsive from non-responsive materials, which is evidenced by the wholesale seizure of Mr.

Klyushin's iCloud accounts, including swaths of data (approximately 380 gigabytes worth), most of it unrelated to this case. *See United States v. Levasseur,* 699 F. Supp. 965, 982 (D. Mass. 1988) (Young, J.), *rev'd in part on other grounds*, 846 F.2d 786 (1st Cir. 1988) ("[S]trong evidence that the warrants were lacking in particularity is provided by the materials actually seized which suggest that the executing agents engaged in a general rummaging."). Accordingly, Mr. Klyushin is entitled to a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978) and the suppression of all fruits, both direct and derivative, of the ensuing searches.[1]

Relying on Special Agent Kang's statement that the affidavit "does not set forth all of [his] knowledge about this matter," Exhibit 1 to Motion at ¶ 9, the government expands its allegations to include details that were previously omitted from Special Agent Kang's affidavits. Specifically, the government alleges there was "abundant probable cause to support the requested search warrant," in part, because Ermakov had placed a trade in Avnet "through Saxo Bank, where Irzak had opened an account and made suspicious trades," as well as the fact that Mr. Ermakov had placed a trade in CFDs when "other traders had sold short before the close of the market …. before Avent's announcement of negative financial news that would make those trades profitable." Opp. at 11.[2] While the September Affidavit states that Irzak opened a Saxo

[1] That Special Agent Kang retired from the FBI on September 30, 2022, does not foreclose his testimony at a *Franks* hearing. According to recent media reports, Special Agent Kang is now the Head of Investigations for crypto exchange Binance, *see https://www.wsj.com/articles/binance-us-hires-high-profile-fbi-agent-as-head-of-investigations-11666278072?*. Nothing indicates that he is unavailable or unwilling to testify.

[2] The Government also labels CFDs "a risky and speculative security." Opp. at 11. The risks associated with purchasing or selling CFDs, however, are no greater than purchasing or selling

Bank account in March of 2018 and alleges that it was "used to engage in suspicious trading," the October affidavit omits that same information. *See* Exhibit 1 to Motion at ¶ 29-32; Exhibit 3. It is unclear based on the omission from the October affidavit whether these allegations contributed to Magistrate Judge Bowler's finding of probable cause in connection with any of the search warrants. Furthermore, both affidavits exclude any details concerning which stocks Irzak's Saxo Bank account traded and whether any overlapped with Mr. Klyushin's transactions (including Avnet). The affidavits and the opposition also omit information that would have further decoupled any connection between the use of Saxo Bank by Mr. Klyushin and Irzak: that Mr. Klyushin did not open an account with Saxo Bank until June of 2019 whereas Irzak opened his account some 16 months earlier in March of 2018, and Irzak did not use the Saxo Bank account (instead using an Interactive Broker account) to place his Avnet transaction.[3]

The additional contention that Mr. Klyushin's Avnet transaction occurred before "negative financial news that would make [Irzak's short positions and Klyushin's CFD positions] profitable" is also wrong. Opp. at 11. On January 23, 2020, Avent published a mixed earnings report stating it beat its revenue expectations but missed its earnings estimate. *See https://seekingalpha.com/news/3534189-avnet-reports-mixed-q2-inline-guide*. The earnings report caused Avnet's stock price to increase the following day, *see* Exhibit 6 to Motion, which

---

the underlying shares of a security. *See https://www.contracts-for-difference.com/Margin-trading-risky.html* ("In other words the risk is identical whether you buy 1000 [] shares or take out a contract for difference controlling 1000 [] shares.").

[3] In essence, anyone shorting or using a derivative product to bet on the decline of Avnet's share price on January 23, 2020, could have been a target of the government's investigation and subject to the wide-spread searches and seizures here.

would have made Irzak's and Mr. Klyushin's transactions unprofitable. Indeed, Mr. Klyushin held the Avnet position for three days, selling it on January 27, 2020. Irzak, on the other hand, covered his approximate $500,000 short position on January 24, 2020, for a loss of approximately $15,000 (or 3% of the total transaction). If the details of Avnet trading were fully and fairly disclosed in Agent Kang's affidavit, they would have shown the antithesis of parallel trading based on an early preview of the Avnet earnings report. Why would any rational trader short the stock or sell CFDs for ensuing losses upon seeing a significantly favorable report if, as the government alleges, the report had been accessed prior to announcement? Exhibit 1 to Motion at ¶ 26.

The government similarly adds information to justify Special Agent Kang's statement in the September affidavit that Mr. Klyushin was "believed to have traded in parallel with IRZAK in multiple publicly traded companies generally within hours of earnings announcements" Exhibit 1 to Motion at ¶ 38. The government cites a November 26, 2019, email from the SEC that contains a spreadsheet of 20 individuals with a cover letter stating, "[p]ursuant to your access letter request – please see the following compiled information." There is no additional information that can be gleaned from the cover email or attachment that would indicate it was intended to be a list of "parallel and suspicious trading ahead of corporate earnings announcements." Opp. at 13. It is also unclear whether Special Agent Kang ever reviewed the spreadsheet and which transactions (if any) the spreadsheet is based on or whether it truly

represents evidence that these accounts engaged in "parallel" trading.[4] Regardless, this Honorable Court should not rely on evidence outside the four corners to rescue such deficient affidavits. *See United States v. Vigeant*, 176 F.3d 565, 569 (1st Cir. 1999) (review properly limited to "information provided in the four corners of the affidavit supporting the warrant application."); *United States v. Zayas-Diaz*, 95 F.3d 105, 111 (1st Cir. 1996) ("The issuing magistrate ordinarily considers only the facts set forth in supporting affidavits accompanying the warrant application."); *United States v. Austin*, 991 F.3d 51, 55 (1st Cir. 2021) (limiting review to "the 'facts and supported opinions' set out within the four corners of the affidavits").

Alternatively, the government, relying on the October affidavit that still resulted in issuance of the iCloud warrant, *see* Exhibit 4 to Motion, argues that Agent Kang's beliefs concerning Mr. Klyushin's engagement in parallel trading with Irzak and others is immaterial to probable cause. This, however, only begs the question: probable cause for and as to *what*?

"Probable cause exists when 'the affidavit upon which a warrant is founded demonstrates in some trustworthy fashion the likelihood that an offense has been committed and that there is sound reason to believe that a particular search will turn up evidence of it.'" *United States v. Schaefer*, 87 F.3d 562, 565 (1st Cir. 1996) (quoting *United States v. Aguirre*, 839 F.2d 854, 857–58 (1st Cir. 1988)). "Mere suspicion, rumor, or strong reason to suspect wrongdoing are not sufficient." *United States v. Vigeant*, 176 F.3d 565, 569 (1st Cir. 1999) (internal citations and quotations omitted). Stripped of the statements the government dubs "immaterial" (*i.e.*, statements

[4] The fact that these questions remain unanswered is another principled reason for this Honorable Court to hold an evidentiary hearing.

concerning Special Agent Kang's beliefs of parallel trading with Irzak in multiple publicly traded companies), no evidence in the September or October 2020 affidavits links Ermakov or Mr. Klyushin to the unauthorized intrusion of Filing Agent 1 and 2 or to broader parallel trading in publicly traded stocks with Irzak and others. The only relevant allegation relating to the unauthorized intrusion of Filing Agents 1 and 2 is Ermakov's stale, unrelated indictments in July and October 2018 for other computer hacking and that he had placed a transaction in one stock serviced by Filing Agent 1 in Mr. Klyushin's Saxo Bank account two days after that report and numerous other stock reports were allegedly accessed. There are no allegations that Ermakov or Mr. Klyushin ever spoke with Irzak or that they otherwise engaged in widespread parallel trading with him or others if, as the government contends, Special Agent Kang's beliefs were immaterial – a belief that was crucial to asserting probable cause beyond Avnet. The remaining evidence included unspecified WhatsApp communications between Ermakov and Mr. Klyushin from May 29, 2020, through July 9, 2020, and a calendar entry that Special Agent Kang again "believes" relates to a meeting between Ermakov and Mr. Klyushin on March 27, 2019. This is the sort of speculation that should not have resulted in the broad warrants that issued. *See. Vigeant*, 176 F.3d at 571 (1st Cir.1999) ("we focus on the facts and supported opinions in the affidavit, ignoring unsupported conclusions.") (internal citation and quotations omitted). The defense respectfully submits these facts are insufficient to establish probable cause that any of the target offenses were committed or that any evidence was foreseeably located in Mr. Klyushin's iCloud account. Special Agent Kang's speculation regarding the possibility of some criminal conduct based on the otherwise innocuous allegations does not usurp this Court's role in weighing the underlying factual content per the

prevailing probable cause standard. *See United States v. Ventresca*, 380 U.S. 102, 109 (1965) ("Recital of some of the underlying circumstances in the affidavit is essential if the magistrate is to perform his detached function and not serve merely as a rubber stamp for the police."); *Aguilar v. Texas*, 378 U.S. 108, 113 (1964) (stating that the magistrate "must judge for himself the persuasiveness of the facts relied on by a complaining officer to show probable cause" (citation omitted)). Even assuming *arguendo*, the two affidavits established probable cause, at most they established probable cause to search for evidence relating to one stock – Avent. The search warrants, however, extended well beyond this one stock or the time frame of the purported intrusion and trading relating to it, allowing government agents to rummage through an entire iCloud account to fish for evidence they hoped would support their investigation. *See* Exhibit 2 and 4 to Motion (authorizing seizure of 19 categories of evidence from January 1, 2018, to the present). Because no reasonable officer could have believed in the validity of a warrant that purported to authorize the search and seizure of Mr. Klyushin's entire iCloud account based on the proffered probable evidence, any materials seized beyond the scope of whatever probable cause this Court determines to have existed must be suppressed. Of course, if the Court finds no probable cause, the entire fruits of the searches must be suppressed.

As to Special Agent Kang's withholding prior omissions and misstatements in a separate high-profile insider trading case, Agent Kang made the considered decision to exclude evidence and analyses from his affidavits, resting the entire proposition that Mr. Klyushin traded in parallel with Irzak and others "in multiple publicly companies generally within hours of earnings announcements" solely on his own unsourced beliefs. In *United States v. Rajaratnam*, Judge

Holwell denied the *Franks* hearing request only because of ample untainted probable cause. In *United States v. Southard*, the court similarly determined there was sufficient probable cause even absent the misstatements. 700 F.2d 1, 9 (1st Cir. 1983) ("Even if we assume that these particular misstatements were knowing and intentional—a large assumption—they are irrelevant to the finding of probable cause."). The district court in *Southard* ultimately denied a request for a *Franks* hearing; instead, the court interviewed the agent in an ex parte, *in camera* proceeding to "protect the fourth amendment rights of defendants while keeping the identity of the informants secret." *Id.* at 11. Informant safety considerations aren't an issue here. An adversarial evidentiary hearing would better serve the purpose of determining whether Special Agent Kang had support for his beliefs or whether he lacked any and wanted to fish for one as backfill and excluded prior credibility reservations to ensure the warrant issued. The fact is Special Agent Kang proffered no evidence tying Mr. Klyushin to a broad insider trading scheme. The sole Avnet transaction, as more fully discussed above, was the antithesis of parallel insider trading. Special Agent Kang, attempting to fix the evidentiary gap, put his own credibility in issue by making his unsourced beliefs central to the determination of probable cause beyond Avnet. No court could fairly evaluate the plausibility of his unsourced beliefs – could intelligently determine if they merited acceptance, reliance and trust – in a vacuum, without a full picture of the bona fides of the agent professing them. Agent Kang gave Magistrate Bowler a selective, incomplete and slanted one. Even the extrinsic explanation the government adds to justify his belief – the SEC spreadsheet from November of 2019 containing 20 names including Irzak and Mr. Klyushin – leaves more questions than answers. The government alleges that it was a spreadsheet evidencing "parallel

and suspicious trading ahead of corporate earnings announcements." Opp. at 13. It is unclear whether Special Agent Kang reviewed the spreadsheet, what information and analyses it is based on, and whether it evidenced any parallel trading. Here, probable cause as to all but Avnet turned solely on Agent Kang's unsourced belief, and Judge Holwell's reservations about his candor plainly bore on whether Magistrate Judge Bowler should credit his naked belief. Special Agent Kang's omissions were deliberate, as evidenced by the above omissions regarding the Avnet transaction which would have removed it from the heartland of parallel insider trading. Indeed, it was not timely, parallel, or profitable. Failing to make disclosures that would negate the credibility of that belief, while at the same time touting the agent's reputation and experience investigating federal wire fraud and insider trading charges, warrant the requested *Franks* hearing.

Finally, the two warrants issued for Mr. Klyushin's iCloud accounts authorized the government to seize Mr. Klyushin's iCloud in a two-step procedure that permitted an unprecedented fishing expedition resulting in the seizure of nearly 380 gigabytes of data, including records dating as far back as May of 2005.

First, both warrants commanded Apple to produce limitless records of

(1) images, videos, audio, documents and files;
(2) address book information;
(3) other stored electronic information (including complete backups of WhatsApp text messages, video messages, audio files, documents and contacts);
(4) records of account registration (including credit card and bank account numbers, IP addresses, cookies, server logs);
(5) all records regarding the devices associated with or used in connection with the

account;

(6) subscriber data and login history;

(7) all location data;

(8) all files and keys necessary to decrypt data;

(9) All find My iPhone connection logs and transactional activity;

(10) All accounts linked to the iCloud account; and

(11) All backup copies.

Additionally, the search warrants required Apple to produce data from "January 1, 2018, to the present" containing:

(1) messages content;

(2) instant message content;

(3) iCloud data including app data, photos and audio files;

(4) online searches and browsing history;

(5) all records and other information concerning files created or accessed by the user of the account;

(6) all records of communication between Apple and the user of the account.

Exhibit 2 to Motion at 2-6; Exhibit 4 to Motion at 2-6.

Second, the warrants required law enforcement personnel to conduct targeted seizures for the following evidence:

> For the period January 1, 2018 to the present, all information described above in Section II that constitute evidence, fruits, or instrumentalities of offenses including wire fraud, in violation of Title 18, United States Code, Section 1343; conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349; fraud and related activity in connection with computers, in violation of Title 18, United States Code, Section 1030(a)(4); money laundering and conspiracy to commit money laundering, in violation of Title 18, United States Code, Section 1956; securities fraud, in violation of Title 15, United States Code 78j(b) and 78ff(a); and conspiracy to commit securities fraud, in violation of Title 18, United States Code, Section 371, including records in any form relating to the following:

1. Material, non-public information ("MNPI") regarding publicly traded companies and/or tending to discuss or establish the possession of MNPI, or from whom MNPI was obtained;

2. Benefits received or provided in exchange for MNPI;

3. The existence of a personal relationship between or among MIKHAIL IRZAK, IGOR SLADKOV, ALEXANDER Redacted, EVGENY Redacted OLGA Redacted, IVAN ERMAKOV, VLADISLAV KLIUSHIN, AREG Redacted, ALEX Redacted (the "Target Subjects"), and/or others with access to MNPI;

4. Documents or communications concerning the existence of a fiduciary duty and/or a duty of trust and confidence owed by the Target Subjects or any user of the Target Account to any person or entity with MNPI regarding publicly traded companies;

5. Saxo Bank, Zerich Securities Limited, Millennium bcp, BrokerCreditServices, and other banks;

6. Actual or contemplated business transactions or corporate announcements by any publicly traded companies;

7. Transactions conducted or contemplated in publicly traded companies, as well as evidence of the ownership and control over the brokerage accounts used to conduct such transactions;

8. Brokerage accounts, other e-mail addresses, social media accounts, messaging app accounts, and/or phone numbers used by: the Target Subjects, the individual(s) controlling or using the Target Account, or other individuals who traded in publicly-traded companies, or individuals who received or had access to MNPI regarding publicly-traded companies;

9. Intrusions into corporate networks including data derived from such intrusions.

10. Filing agents for publicly traded companies;

11. File-sharing applications or other ways to exfiltrate or send data;

12. The identity of any individual who accessed or controlled the Target Account;

13. The existence, identity, and location of any co-conspirators of the Target Subjects or any other user of the Target Account;

14. Evidence of the geographic location of user(s) of the Target Account, as well as the identity and location of computers or devices used to access the Target Account;

15. The past travel or whereabouts of the person or persons who have owned, controlled, or operated the Target Account;

16. Evidence of the establishment and use of bank accounts to transfer the proceeds of insider trading in publicly traded companies;

17. Other e-mail or Internet accounts providing Internet access or remote data storage to any Target Subject or user of the Target Account;

18. The existence or location of physical media storing electronic data, such as hard drives, CD- or DVD-ROMs, or flash drives; and

19. The existence or location of paper print-outs of any data from any of the above.

B. All of the subscriber, transactional, and logging records described in Section II(B).

Exhibit 2 to Motion at 7-9; Exhibit 4 to Motion at 7-9.

This seize now, narrow later approach appears to be a regular practice by the United States Attorney's Office in this District. *See, e.g., United States v. Kanodia*, No. 15-CR-10131, 2016 WL 3166370, at *6-7 (D. Mass. June 6, 2016); *United States v. Aboshady*, 951 F.3d 1, 5 (1st Cir. 2020) (authorizing Google to turn over entire email account, followed by a filtration team review, and then review by the investigative team). But the legal authority used to justify the procedure is far afield from the present context involving seizure of an entire iCloud account. In *United States v. Upham*, 168 F.3d 532 (1st Cir. 1999), officers executing a search warrant on the defendant's home seized his computer. The First Circuit rejected a defense argument that the

warrant purporting to authorize such seizure lacked particularity because, "[a]s a practical matter, the seizure and subsequent off-premises search of the computer . . . was about the narrowest definable search and seizure reasonably likely to obtain" the suspected child pornography. *Id.* at 535. Technology has advanced in the more than two decades since *Upham*, such that wholesale seizure of electronic evidence is sometimes far from the narrowest practical alternative.

In the circumstances of this case, where Mr. Klyushin's data was remotely accessible via his iCloud account, there was no evident reason why the government could not have constructed a narrower set of demands consistent with the scope of probable cause, which as discussed in detail above was quite limited to the extent it existed at all. Indeed, one district court has distinguished *Upham* and other similar cases from other circuits on the grounds that they "addressed the search of computers and hard drives, not email accounts." *United States v. Matter of Search of Info. Associated With Fifteen Email Addresses Stored at Premises Owned*, No. 17-CM-3152, 2017 WL 4322826, at *6 (M.D. Ala. Sept. 28, 2017). "'[H]ard drive searches require time-consuming electronic forensic investigation with special equipment' due to the myriad ways one can hide evidence on a hard drive. 'By contrast, . . . when it comes to [online] account searches, the government need only send a request with the specific data sought and [the vendor] will respond with precisely that data.'" *Id.* (*quoting United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017)).

On the other side of the constitutional balancing, namely the privacy implications of the search, a great deal has changed since *Upham* was decided in 1999. As the First Circuit and Supreme Court recognized almost a decade ago, "[t]he storage capacity of today's cell phones is immense." *United States v. Wurie*, 728 F.3d 1, 8 (1st Cir. 2013); *Riley v. California*, 573 U.S. 373,

394, (2014) ("a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. … . The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet."). And the devices are "increasingly" used to "store personal user data in the cloud instead of on the device itself." *Id.* n.8 (citation omitted). "That information is, by and large, of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web searching and browsing history, purchases, and financial and medical records." *Id.* In short, "[j]ust as customs officers in the early colonies could use writs of assistance to rummage through homes and warehouses, without any showing of probable cause linked to a particular place or item sought," the government's practice of seizing entire iCloud accounts belonging to those suspected of criminal wrongdoing improperly results in "automatic access to a virtual warehouse of an individual's most intimate communications and photographs without probable cause" tied to those specific materials. *Id.* at 9 (citation omitted); *see also United States v. Lofstead*, 574 F. Supp. 3d 831, 839 (D. Nev. 2021) ("District courts nationwide have begun expressing concerns about over-searching ESI, especially because warrants often authorize the government to seize large quantities of personal information that it lacks probable cause to search."). This runs afoul of the Supreme Court's command to "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *United States v. Jones*, 565 U.S. 400, 406 (2012) (citation omitted).

Even assuming, contrary to the foregoing, that the particularity requirement does not apply to the initial seizures of Mr. Klyushin's iCloud account, the categories of materials subject to search listed in both warrants were "so numerous and unspecific to create an [effectively] unrestricted dragnet search." *Lofstead*, 574 F. Supp. 3d at 844 (citation omitted). At best, assuming there was probable cause to believe any crime had been committed, the scope of such probable cause was limited to a single transaction, Avnet. But the scope of the searches purportedly permitted by the warrants was much broader, extending to all "evidence, fruits, or instrumentalities of offenses including [six] offenses…. including records in any form relating [to 19 categories]." Exhibit 2 to Motion at 7; Exhibit 4 to Motion at 7. A commonsense reading of the warrants is that they have no limitations at all. In short, one transaction in Avnet in Mr. Klyushin's account was insufficient to create "probable cause of ongoing or serial criminal incidents." *Lofstead*, 574 F. Supp. 3d at 840-41. The government, therefore, should not have been permitted to leverage an isolated incident of suspected parallel trading into a wide-ranging search for evidence of any other unspecified misconduct. *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) ("[A] serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant. This threat demands a heightened sensitivity to the particularity requirement in the context of digital searches.") (internal citations and quotations omitted).

Agents' execution of the iCloud searches reinforces the overbreadth of the warrants. *See Levasseur*, 699 F. Supp. at 982 ("[S]trong evidence that the warrants were lacking in particularity is provided by the materials actually seized which suggest that the executing agents engaged in a

general rummaging."). The government produced in discovery hundreds of thousands of files that have been extracted from Mr. Klyushin's iCloud account that are not in any way related to this case or the categories of documents the warrants permitted the government to seize. Indeed, the seized documents from Mr. Klyushin's iCloud account includes approximately 380 gigabytes of information that contain the following:

| **Date Range** | **Data Type** | **Quantity of Records** |
|---|---|---|
| December 20, 2014 - October 4, 2020 | Messages (including iCloud messages, Threema messages, and WhatsApp messages) | 130,505 |
| March 31, 2007 - November 12, 2020 | Pictures | 95,114 |
| March 18, 2012 - July 4, 2020 | Location Records | 32,969 |
| May 28, 2005 – November 24, 2020 | Calendar Entries | 3,224 |
| December 25, 2018 – October 4, 2020 | Call logs | 609 |
| April 25, 2016 - October 4, 2020 | Wi-fi Connection Records | 1,270 |
| August 24, 2019 - November 12, 2020 | Audio Recordings | 210 |
| February 10, 2013 - November 12, 2020 | Videos | 4,199 |
| December 14, 2011 - October 10, 2020 | Emails | 2,376 |
| August 21, 2014 - November 12, 2020 | Documents | 3,542 |

Additionally, the government seized application data for 284 iPhone apps, 15,623 contact entries, 1,270 reflecting connections to another device, 175 notes and memorandum, 2575 search and web files, 20,726 system and log files, and 100,000+ other files that that include archives,

configurations, and other "uncategorized" data that was picked up by the government's searches.

This wholesale seizure of Mr. Klyushin's iCloud was unjustified and most, if not all, of the data is irrelevant to the 19 categories law enforcement employed to narrow their seizures. For example, the government seized 11,592 Messages to Mr. Klyushin's wife and 6,128 Messages from Mr. Klyushin's wife. The government similarly seized all messages with Mr. Klyushin's minor son and two minor daughters (including their group chats), communications with friends, and communications with employees. This seizure quite literally resulted in law enforcement, receiving nearly every detail of Mr. Klyushin's life. The irrelevant nature of the seized information is so eminently clear at first glance given they include conversations outside the temporal scope and conversations about extracurricular activities, sports, dinner, photos of family activities and vacations, etc. The government was not shy about using all this seized information against Mr. Klyushin. In its bail filings, the government prominently features a March 5, 2020, invoice for a three million British pound yacht, *see* Dkt. 23 at 4, as well as his November 27, 2017 award from FSB, Dkt. 59 at 5, and his June 2020 medal of honor.[5] The defense respectfully contends none of these items relate to the matters the government had probable cause to search for and seize.

"[T]he remedy in the case of a seizure that casts its net too broadly is" suppression of all materials "that reasonably fell outside the [legally permissible] scope of the warrant." *United States v. Aboshady*, 951 F.3d 1, 9 (1st Cir. 2020) (citation omitted); *see also United States v. Levasseur*,

[5] The dissemination of this information resulted in numerous publications speculating that Mr. Klyushin is a Kremlin insider, *see https://www.bloomberg.com/news/articles/2022-01-03/kremlin-insider-klyushin-is-said-to-have-2016-hack-details*, viewed over 50 million times by some estimates.

704 F. Supp. 1158, 1173 (D. Mass. 1989) (Young, J.). However, "[i]f no portion of the warrant is sufficiently particularized to pass constitutional muster, then total suppression is required. Otherwise the abuses of a general search would not be prevented." *United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982); *In re Grand Jury Investigation Concerning Solid State Devices, Inc.*, 130 F.3d 853, 855 (9th Cir. 1997) (warrant which resulted in the seizure of approximately 90% of corporation's records over a five-year period, required return of all property). The overbreadth of both the warrants at issue and the seizures they spurred demands suppression of *all* evidence confiscated in consequence. Indeed, the warrants at issue, essentially purporting to authorize seizure of Mr. Klyushin's entire iCloud account, were so facially lacking in particularity that "no officer could have reasonably presumed" they were valid. *Levasseur*, 699 F. Supp. 965 at 982. Indeed, a Special Agent with nearly 20 years' experience and seasoned prosecutors, who were concerned by the prospect of extending the government's ability to monitor its citizens' activities, *see* https://www.thecrimson.com/article/1994/3/3/the-return-of-1984-pbhaving-the/, failed "to recognize that the Warrant[s] authorize[d] a general search of [Mr. Klyushin's iCloud]" and other information. *Lofstead*, 574 F. Supp. 3d at 846. "When faced with a warrant that authorizes an unrestricted search of almost all, if not explicitly all, content on a cell phone [or, in this case, an iCloud account], an executing officer behaving in good faith should know that such a search is objectively unreasonable and would likely violate the defendant's Fourth Amendment rights." *Id.* Alternatively, if this Honorable Court believes the categories of evidence to be seized were sufficiently particularized, then the government executed the warrants in "flagrant disregard" of the warrant's terms, similarly requiring full suppression. *United States v. Matias*, 836 F.2d 744, 747

(2d Cir. 1988); United States v. Medlin, 842 F.2d 1194 (10th Cir. 1988); *United States v. Medlin*, 842 F.2d 1194, 1199 (10th Cir. 1988) ("[w]hen law enforcement officers grossly exceed the scope of a search warrant in seizing property, the particularity requirement is undermined and a valid warrant is transformed into a general warrant thereby requiring suppression of all evidence seized under that warrant."). Of course, to the extent this Honorable Court orders suppression because of Special Agent Kang's omissions and misstatements, the good-faith exception is inapplicable. Suppression is intended to deter and disincentivize future violations, "encourag[ing] those who formulate law enforcement policies, and the officers who implement them, to incorporate Fourth Amendment ideals into their value system." *Stone v. Powell*, 428 U.S. 465, 492 (1976). There is no better way to vindicate and promote "Fourth Amendment ideals" than suppressing the evidence in this case – one where an agent who previously made omissions and misstatements continues to skate near or over the line in matters materially affecting credibility to spy on the contents of someone's entire life.

Respectfully Submitted,
Vladislav Klyushin,
By His Attorney,

**/s/ Maksim Nemtsev**
Maksim Nemtsev, Esq.
Mass. Bar No. 690826
20 Park Plaza, Suite 1000
Boston, MA 02116
(617) 227-3700
menemtsev@gmail.com

**/s/ Marc Fernich**
Marc Fernich
Law Office of Marc Fernich
800 Third Avenue
Floor 20
New York, NY 10022
212-446-2346
Email: maf@fernichlaw.com

Dated: October 24, 2022

**CERTIFICATE OF SERVICE**

I, Maksim Nemtsev, hereby certify that on this date, October 24, 2022, a copy of the foregoing documents has been served via Electronic Court Filing system on all registered participants.

**/s/ Maksim Nemtsev**
Maksim Nemtsev, Esq.